Amendment To The Claims

Please amend the claims as follows:

Claim 1: (previously amended) A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

a. receiving input data representing the entire facsimile document and generating facsimile information in a first format by said first communication device from said input data;

b. processing said input data, at said first communication device, to compute an encrypted checksum of the entire input data;

c. convolving said facsimile information with said encrypted checksum data to produce convolved data;

d. decrypting, at said second communication device, said encrypted checksum;

e. computing a checksum of said input data received at said second communications device; and

f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d) by clearly marking the received input data indicating a tamper condition.

Claims 2-4 (Canceled).

Claim 5: (previously amended) The method of claim 1, wherein a database system is communicatively coupled to said second facsimile communication device.

Claim 6 (Canceled).

Claim 7: (previously amended) The method of claim 1, further comprising the step of configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data.

Claims 8-9 (Canceled).

Claim 10: (previously presented) The method of claim 1, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes printing a clear mark across a print out of the received input data indicating a tamper condition.

Claim 11: (previously presented) The method of claim 1, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition.

Claim 12: (previously presented) The method of claim 1, wherein the convolved data is transmitted to the second facsimile communication device as an e-mail attachment.

Claim 13: (previously presented) The method of claim 1, further comprising: Sending the convolved data to a third facsimile communication device.

Claim 14: (previously presented) The method of claim 1, further comprising:

receiving a user name and password from a user with the second facsimile communication device.

Claim 15: (previously amended) A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the digital representation of the entire facsimile document in a first format sent by said first communication device;

processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data;

decrypting, at said second communication device, said encrypted authentication data;

computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data; and

alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data by clearly marking the received input data indicating a tamper condition.

Claim 16: (previously presented) The method of claim 15, wherein a database system is communicatively coupled to said second facsimile communication device.

Claim 17: (previously presented) The method of claim 15, further comprising the step of configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data.

Claim 18: (previously presented) The method of claim 15, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes printing a clear mark across a print out of the received input data indicating a tamper condition.

Claim 19: (previously presented) The method of claim 15, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition.

Claim 20: (previously presented) The method of claim 15, wherein the convolved data is transmitted to the second facsimile communication device as an e-mail attachment.

Claim 21: (previously presented) The method of claim 15, further comprising: sending the convolved data to a third facsimile communication device.

Claim 22: (previously presented) The method of claim 15, further comprising: receiving an authorized user name and password from a user with the second facsimile communication device before providing access to the facsimile document.

Claim 23: (currently amended) A method of authenticating a facsimile document communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

receiving at the second facsimile communications device transmitted data including a digital representation of the entire facsimile document and convolved encrypted authentication data associated with the facsimile document and consisting of a single encrypted checksum of the entire facsimile document in a first format sent by said first communication device;

processing said transmitted data, at said second communication device, to extract a digital representation of the entire facsimile document and convolved encrypted authentication data;

decrypting, at said second communication device, said encrypted authentication data;

computing, at said second communication device, a comparison version of the authentication data using the a digital representation of the entire facsimile document and convolved encrypted authentication data; and

alerting a recipient at said second communication device in the event of a mismatch between said authentication data and said comparison version of the authentication data,

wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes printing a clear mark across a print out of the received input data indicating a tamper condition.

Claim 24: (canceled).

Claim 25: (previously presented) The method of claim 23, wherein the step of alerting the recipient at said second facsimile communication device in the event of a mismatch includes displaying a clear mark across a computer display of the received input data indicating a tamper condition.